REMARKS/ARGUMENTS

This Reply is submitted in response to the final
Office Action dated October 24, 2007. The deadline for
responding is January 24, 2008.

I.   Introduction

Claims 1-14 are now pending. In the Office Action
the Examiner rejected claims 1-7 and 9-13 under 35 U.S.C.
§103(a) as being unpatentable over U.S. Patent
Publication No. 2003/0195861 to McClure et al.
(hereinafter "the McClure et al. publication") in view of
U.S. Patent Publication No. 2003/0115321 to Edmison et
al. (hereinafter "the Edmison et al. publication"). In
addition the Examiner rejected claims 8 and 14 under 35
U.S.C. §103(a) as being unpatentable over the McClure et
al. publication in view of the Edmison et al. publication
, and further in view of U.S. Patent Publication No.
2004/0028035 to Read (hereinafter "the Read
publication").

As will be discussed below, none of the pending
claims are rendered obvious by the applied references.

II.   The Rejections under §103

Claim 1 discloses (emphasis added):

> *A method of testing a network firewall,
> comprising:*
>   ***transmitting a communications session
> initiation signal from said signal source using
> an IP address corresponding to said signal
> source to establish a communications session to
> be conducted through said firewall;***
>   ***transmitting test signals from said signal
> source, following initiation of said
> communications session and prior to termination***

7

of said initiated communications session, at a range of ports in a first side of said firewall through which media signals may be transmitted when said ports are open, said test signals including said IP address;

monitoring a second side of said firewall to detect any transmitted test signals that pass through said firewall; and

identifying any open ports that are not associated with said established communications session, which passed at least one of said transmitted test signals, as erroneously open ports.

The Examiner acknowledges on p. 3 of the Office Action that:

"McClure et al. does not teach ….a second test device located on a trusted side of said firewall, the second test device including: means for monitoring a second side of said firewall to detect any transmitted test signals that pass through said firewall and an analysis module for identifying any open ports that are not associated with an established communications session, which passed at least one of said transmitted test signals, as erroneously open ports."

The Examiner goes on to state that (emphasis added):

"Edmison et al. teaches … a second test device located on a trusted side of **said firewall**, the second test device including (fig. 1, ref. num 10 and 20): means for monitoring a second side of **said firewall** to detect any transmitted test signals that pass through **said firewall** (paragraph 0040) and **an analysis module for identifying any open ports that are not associated with an established communications session, which passed at least one of said transmitted test signals, as erroneously open ports** (paragraph 0010)."

First, there is no mention of a **firewall** in the cited references of the Edmison et al. publication. Fig.

8

1 shows a "first network element" 10; and a "second
network element 20", a "user card 31", and a "user
destination 29" at the distant end of the network being
tested. Fig. 2 shows a "network element" 10, with
"ingress user port(s)" 52 and 54, and "egress user
port(s)" 49 and 56. There is no mention of "firewalls".
Neither paragraph 10 nor paragraph 40 mentions a
"firewall".

The Edmison et al. publication discloses (abstract):

> "a method which involves inserting probe
> packets on a per service basis for transmission
> on a respective round trip; and for each
> service using the probe packets to calculate
> packet latency for probe packets which is
> representative of packet latency for all
> packets transmitted for the service. In some
> embodiments, data plane time stamps are used to
> accurately time probe latency. The invention
> also provides a method which involves inserting
> probe packets on a per service basis for
> transmission on a respective destination
> network element; and at the destination network
> element for a given service using the probe
> packets to calculate one way packet loss for
> the service".

As can be seen, the Edmison et al. publication
teaches sending probe packets to a destination and back
to the origination, while monitoring to see how long this
process takes, and whether any packets are dropped.
There is no suggestion of testing a **firewall**.

The Examiner states on page 8: "the word firewall
does not need to appear so long as there is an item that
acts and behaves like a firewall present in the network".
The Examiner also states: "McClure is the reference cited

9

for actually teaching testing a firewall, as shown in figure 1." Applicant continues to maintain that the Edmison et al. publication tests network latency by sending and receiving probes from various places in a network, without targeting (or even mentioning) firewalls. Therefore, it does not follow that the McClure et al. publication teachings would be incorporated into the Edmison et al. publication teachings for "*monitoring a second side of said firewall to detect any transmitted test signals that pass through said firewall*".

Second, there is no teaching or suggestion in the Edmison et al. publication of "***identifying any open ports that are not associated with said established communications session***". The Edmison et al. publication discloses, at paragraph 0040:

> "Each packet received at an ingress user port belonging to a given service is typically given a certain treatment, and forwarded to an appropriate egress network port. A count of these packets is maintained for each service."

It can be seen that ports are selected for use as ingress and egress ports for probe packets, and there is no teaching or suggestion of looking for or identifying open ports **of a firewall that are not associated** with the testing probe transmissions and receptions ("established communications session").

Further, there is no teaching or suggestion in the Edmison et al. publication of identifying any ports "***as erroneously open ports***". There is no mention of "erroneously open ports" in the Edmison et al. publication, to say nothing of "identifying" them.

10

Neither the McClure et al. publication nor the
Edmison et al. publication teach or suggest the features
of claim 1 of:

> ***identifying any open ports that are not
> associated with said established communications
> session,*** which passed at least one of said
> transmitted test signals, ***as erroneously open
> ports***

Therefore, no combination of the McClure et al.
publication and the Edmison et al. publication teach or
suggest the above feature of claim 1.

The Examiner states on page 8: "McClure teaches, at
paragraph 0130, that TCP packets are sent to all ports
and packets that get a timeout are in response to closed
ports." The Examiner then states, regarding the Edmison
et al. publication: "The packets are considered erroneous
when they non-conform". However, neither statement
refers to "erroneously open ports". The McClure et al.
publication teaches identifying open ports, and the
Edmison et al. publication identifies non-conforming
packets. Therefore, no combination of the references
teaches or suggests "*identifying any open ports that are
not associated with said established communications
session, which passed at least one of said transmitted
test signals, as erroneously open ports*".

Further, the McClure et al. publication teaches
testing ports by sending signals toward the ports, and
identifying **responses to those signals from the target
device.** At paragraph 11 it states: "The system and
method can be run remotely from a monitoring computer
outside the target network, or can be run by a monitoring
computer included within the target network".

11

The Edmison et al. publication teaches transmitting and receiving probes at various places in the network, in order to determine network latency (with associated timing functionality). However, practitioners of the McClure et al. publication, knowing of the Edmison et al. publication, would not choose to incorporate the topology of the Edmison et al. publication into their topology. If someone **suggested** to them that they place devices on the second side of each firewall in each target computer, the response would be that there would be no reason to do so, and that such a solution would be **less** economical than the solution taught by the McClure et al. publication.

Further, even if one **wanted** to incorporate the Edmison et al. publication teachings into the McClure et al. publication system, there is no teaching of how the the McClure et al. publication system should be modified to accomplish such an integration of systems.

Third, neither the McClure et al. publication nor the Edmison et al. publication teach or suggest "*transmitting test signals from said signal source, following initiation of said communications session and prior to termination of said initiated communications session*". Both the McClure et al. publication and the Edmison et al. publication teach sending multiple signals simultaneously. Neither teaches or suggests "*transmitting a communications session initiation signal from said signal source using an IP address corresponding to said signal source to establish a communications session to be conducted through said firewall*", followed by "*transmitting test signals from said signal source, following initiation of said communications session and*

12

prior to termination of said initiated communications session".

Further, neither reference teaches "*identifying any open ports that are not associated with said established communications session*". Again, neither the <u>McClure et al.</u> publication nor the <u>Edmison et al.</u> publication teach or suggest identifying open ports that are *not associated with said established communications session*, since neither references teaches a **communications session** separate from the testing signals.

Additionally, neither reference teaches or suggests "*identifying any open ports that are not associated with said established communications session, which passed at least one of said transmitted test signals, as erroneously open ports*". Neither the <u>McClure et al.</u> publication nor the <u>Edmison et al.</u> publication identify open ports in relation to a specific established communications session in order to identify such open ports as erroneously open ports.

Finally, a feature of claim 1 is (emphasis added): "*transmitting a communications session initiation signal from said signal source* **using an IP address corresponding to said signal source**" and "*said test signals including* **said IP address**". Neither reference teaches or suggests "*transmitting a communications session initiation signal*" "*to establish a communications session to be conducted through said firewall*", "*transmitting test signals*", wherein "*said test signals [include] said IP address*", and "*identifying any open ports that are not associated with said established communications session, which passed at least one of said transmitted test signals, as erroneously open ports*". Neither the <u>McClure et al.</u>

13

publication nor the Edmison et al. publication compares an established communications session with test signal results to identify erroneously open ports. No combination of the references would teach or suggest any of the above features.

For at least these reasons, claim 1 is patentable over the cited references.

Claims 2-8, for at least the reason of being dependent on allowable claim 1, are therefore patentable over the cited references.

Claim 9 contains the following features:

a session signal generator for transmitting a communications session initiation signal using an IP address corresponding to said signal source to establish a communications session to be conducted through said firewall

a probe signal generator for generating test signals at a range of ports in a first side of said firewall through which media signals may be transmitted when said ports are open, said test signals including said IP address

an analysis module for identifying any open ports that are not associated with an established communications session, which passed at least one of said transmitted test signals, as erroneously open ports.

For at least the reasons stated above with regard to claim 1, claim 9 is patentable over the cited references.

Claims 10-14, for at least the reason of being dependent on allowable claim 9, are therefore patentable over the cited references.

14

It should be noted that the Read publication, although not cited against either of independent claims 1 or 9, does not correct any of the deficiencies noted above with regard to the McClure et al. publication and the Edmison et al. publication.

III. Conclusion

In view of the foregoing remarks, it is respectfully submitted that the pending claims are in condition for allowance. Accordingly, it is requested that the Examiner pass this application to issue.

If there are any outstanding issues which need to be resolved to place the application in condition for allowance **the Examiner is requested to call (732-542-9070) and schedule an interview with Applicant's undersigned representative.** To the extent necessary, a petition for extension of time under 37 C.F.R. 1.136 is hereby made and any required fee in regard to the extension or this amendment is authorized to be charged to the deposit account of Straub & Pokotylo, deposit account number 50-1049.

None of the statements or discussion made herein are intended to be an admission that any of the applied references are prior art to the present application and Applicants preserve the right to establish that one or more of the applied references are not prior art.

15

Respectfully submitted,

October 27, 2007

Michael P. Straub

Michael P. Straub Attorney
Reg. No. 36,941
Tel.: (732) 542-9070

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this paper (and any accompanying paper(s)) is being facsimile transmitted to the United States Patent Office on the date shown below.

Michael P. Straub
Type or print name of person signing certification

Michael P. Straub   October 27, 2007
Signature   Date

16